1) authorising [enabling] other software which being protected from unauthorised use, to be used on said computer ; 2) determining the presence of an identity software on said computer ; said [computer use a means for] identity software being for use on said computer to, with no effective protection against unauthorised use, provide [providing] an [encrypted] identity information of [its] the rightful or authorised user of said authorising software, said identity information being for to be authenticated by [to] a remote computer in order for said remote computer to perform operation(s) for which said rightful or authorised user has to be responsible [a secure operation ,] ; and the presence of said identity software on said computer is being determined without a said operation being performed by said remote computer ;

wherein [said software enables the] use of said other software on said computer will be authorised if said [means for providing] identity software is determined as being present on said computer ; and said authorising software and said identity software being software meeting said existing standard ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said protected software ~~thereon~~.

B1 cont

2.(Second time amended) Authorising software, stored in a device or physically on a medium, [Software] as claimed in claim 1, wherein comprising [means] software, when being executed, for determining data integrity of said [means for providing] identity software ; and if the determination is unfavourable, said [means for providing] identity software will further be [regarded] determined as not present.

3.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 1, wherein comprising [means] authenticating software for, when being executed, authenticating said computer ; said authenticating software comprises a stored information of configuration of said

computer and [means] software for, when being executed, determining configuration of said computer and [means] for comparing the determined result with said stored information ; and if [said means for providing is not present on said computer or] the comparison result is unfavourable, said authorising software will not [enable the] authorise use of said other software on said computer.

4.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 3, wherein said configuration of said computer includes the hardware configuration thereof.

5.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 3, wherein said configuration of said computer includes the software configuration thereof.

B1 cont

6.(Second time amended) Authorising software, stored in a device or physically on a medium, [Software] as claimed in claim 3, wherein further comprising a method, comprises the steps of :

receiving [an encrypted] a command from said remote computer ;

authenticating said [encrypted] command ;

determining the hardware or software or both configuration of said computer;

storing the [determinated] determined configuration if the authentication result of said authenticating step is favourable ;

thereafter, determining at least a part of the configuration of a computer onwhich said software runs ;

comparing said at least a part of configuration determined with the corresponding part in said stored configuration ;

authorising [enabling the] use of said other software if the comparison result is favourable.

7.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 6, wherein said [encrypted] command is being entered into said computer by the computer user who receives it from said remote computer through telephone line.

9.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 1, wherein said other software comprises an information stored at a first predetermined location therein for indicating an valid identity of its rightful user exists at a second predetermined location therein and an encrypted identity of its rightful user at a respective location therein ; and said other software, when being executed, will fail to operate if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

10.(Second time Amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 9, said authorising software also comprises said information at said first predetermined location therein and an identity of its rightful user at said second predetermined location therein and an encrypted identity of its rightful user therein ; and said authorising software will not [enable the] authorise use of said other software on said computer if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

11.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 9, wherein comprising an encrypted identity of its rightful user ; and if said other software stored in said computer has a valid user identity not consistent with said encrypted identity in said authorising software, said authoring software will not [enable the] authorise use of said other software.

SUB I2

12.(Second time amended) ~~Software, stored in a device or physically on a medium, for~~ use on a computer which being made to meet an existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof , [for restricting other software to be used on said computer only] , comprising :

[means for providing an encrypted] identity software for use on said computer to, with no individual and effective protection, provided by execution of said software, against unauthorised use, provide an identity information of the rightful or authorised [its] user of an authorising software, said identity information being for to be authenticated by [to] a remote computer in order for said remote computer to perform [a secure operation] operation(s) for which said rightful or authorised user has to be responsible ;

B2 cont

[means for enabling] said authorising software being for, when executed, authorising [enabling the] use of [said] other software which being purchased and being protected from unauthorised use, on said computer ;

Wherein said [means for providing] identity software and said [means for enabling] authorising software are contained in [a] said software [program so as for preventing] in such a manner that said [means for enabling] authorising software is prevented from being copied therefrom individually ; and said authorising software and said identity software being software meeting said existing standard ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said protected software thereon.

13.(Second time amended) Software, stored in a device or physically on a medium, as claimed in claim 12, wherein said other software comprises an information stored at a first predetermined location therein for indicating a valid identity of its rightful user exists at a second predetermined location therein and an encrypted identity of its

rightful user at a respective location therein ; and said other software, when being executed, will fail to operate if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

14.(Second time amended) Software, stored in a device or physically on a medium, as claimed in claim 13, wherein said [means for enabling] authorising software also comprises said information at said first predetermined location therein and an identity of its rightful user at said second predetermined location therein and an encrypted identity of its rightful user therein ; and said [means for enabling] authorising software will not [operate] authorise use of said other software if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

15.(Second time amended) Software, stored in a device or physically on a medium, as claimed in claim 13, wherein further comprising an encrypted identity of its rightful user ; and if said other software stored in said computer has a valid user identity which being not consistent with said encrypted identity in said software, said [means for enabling] authorising software will not [enable the] authorise use of said other software.

16.(Second time amended) Software, stored in a device or physically on a medium, as claimed in claim 12, wherein [further comprising means for authenticating] said authorising software [said computer,] comprises [a stored configuration information] [of said computer and means for determining configuration of said computer and] [means for comparing the determined result with said stored information, and if the] [comparison result is unfavourable, said means for enabling will not enable the use of] said [other] identity software [on said computer].

17.(Second time amended) Authorising software, stored in a device or physically on a medium and meeting an existing standard, [Software] for use on a computer which being made to meet said existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof ; said authorising software being for, when being executed, authorise [enabling] other software which being protected from unauthorised use, to be used on said computer ; [said computer uses a means for providing an encrypted identity of its user to a remote computer for a secure operation;]

wherein a same encryption algorithm [is] used by [said] a means for providing an [encrypted] identity information of the rightful or authorised user of said authorising software, [and] exists in said authorising software and being accessible or, when said authorising software being executed, usable by a user ; said identity information being for to be authenticated by a remote computer in order for said remote computer to perform operation(s) for which said rightful or authorised user has to be responsible ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said other software thereon.

18.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 17, wherein comprising [means] authenticating software for, when being executed, authenticating said computer ; said authenticating software comprises a stored configuration information of said computer and [means] software for, when being executed, determining configuration of said computer and [means for] comparing the determined result with said stored information ; and if the comparison result is unfavourable, said authorising software will not [enable] authorise use of said other software.

19.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 17, wherein said other software comprises an information stored at a first predetermined location therein for indicating a valid identity of its rightful user exists at a second predetermined location therein and an encrypted identity of its rightful user at a respective location therein ; and said other software, when being executed, will fail to operate if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

20.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 19, said authorising software also comprises said information at said first predetermined location therein and an identity of its rightful user at said second predetermined location therein and an encrypted identity of its rightful user therein ; and said authorising software will not [enable] authorise use of said other software if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

21.(Second time amended) [Software] Authorising software, stored in a device or physically on a medium, as claimed in claim 19, wherein comprising an encrypted identity of its rightful user ; and if said other software stored in said computer has a valid user identity not consistent with said encrypted identity in said authorising software, said authorising software will not [enable] authorise use of said other software.